

TABLE OF CONTENTS

Cybersecurity	2
Advanced DNSSEC infrastucture	2
Cybersécurité : Démystification, Opportunités et Défis pour une Carrière d'Avenir	2
Cybersecurity Awareness and the Psychology Behind It	3
Ethical Hacking with Zenmap: Essential Network Scanning Techniques for Ethical Hackers	3
Introduction à la Cybersécurité	4
Introduction to the Domain Name System	5
Learning Track - Cybersecurity Essentials	5
Microsoft Security, Compliance, and Identity Fundamentals	5
Module 2: Network and security - Advanced level	6
Module 3: Security Incident Management	7
Module 4: Incident Response Principle	7
Module 5 - Part 1: Application security - Level 1 - Introduction to Secure Coding	8
Module 5 - Part 1: Application security - Level 2 - Attacks and defenses in action	9
Module 5 - Part 1: Application security - Level 3 - Introduction to Application Security Audits	9
Module 5 - Part 2 : DevOps and Pipeline Security	10
Module 6: Malware and Forensics	11
Multi-factor Authentication	11
Network Security and Intro to Threat Hunting with Wireshark	12
Operating a DNS authoritative service	12
Operating a DNS resolution service	13
Principles of the Domain Name System Security Extensions (DNSSEC)	13
Sensibilisation à la sécurité de l'information	14
TCP/IP Deep Dive for Practioners with Wireshark	14

CYBERSECURITY



ADVANCED DNSSEC INFRASTRUCTURE

Domain Name System Security Extensions (DNSSEC) adds origin authentication and integrity protection to the protocol by signing DNS data. However the ratio of signed domain names remains low, mostly because, as any security feature, DNSSEC brings some risks when implemented without a proper understanding.

This course targets IT students, professionals or enthusiasts currently managing domain names and potentially already signing their DNS zones. It will give them a hands-on experience of reliably operating DNSSEC zone signature in a more reliable and advanced infrastructure.

[View online](#)

Price: 28,00 €

Start date: 13.12.2024

Instructor(s): Dr. HERBIET Guillaume-Jean

Language: English

Difficulty: Advanced



CYBERSÉCURITÉ : DÉMYSTIFICATION, OPPORTUNITÉS ET DÉFIS POUR UNE CARRIÈRE D'AVENIR

Le monde d'aujourd'hui offre de vastes opportunités professionnelles et business, mais expose également de nombreux faiblesses pouvant être exploitées par des personnes malveillantes. La cybersécurité est désormais reconnue comme une préoccupation majeure des conseils d'administration des entreprises. L'image stéréotypée d'un geek avec un sweat noir à capuche et tapant à toute vitesse sur son clavier avec des gants noirs ne reflète pas toute l'étendue offerte par cybersécurité : il s'agit d'un domaine offrant un grand nombre d'opportunités qui vont bien au-delà de ces stéréotypes.

Si vous souhaitez contribuer à rendre Internet plus sûr et donc par effet de rebond à améliorer la sécurité de la Société ; si vous êtes intéressé à travailler dans un domaine en constante évolution ; si vous recherchez une formation continue avec une certitude de débouché ; une carrière dans le secteur de la cybersécurité vous apportera tout cela, et bien plus encore.

Cette formation démystifiera la cybersécurité, en explorant l'étendue de ses sujets et des opportunités de carrière. Nous approfondirons les défis et les opportunités offertes sur le marché, nous parlerons de gestion de crise, de stratégies efficaces et des opportunités émergentes, ainsi que la préparation aux entretiens pour les postes de cybersécurité.

[View online](#)

Price: 12,00 €

Start date: 26.11.2024

Instructor(s): Cédric MAUNY

Language: French

Difficulty: Beginner

CYBERSECURITY AWARENESS AND THE PSYCHOLOGY BEHIND IT

This course delves into the critical role of human behavior in cybersecurity, exploring the psychological factors that influence how individuals interact with technology and respond to cyber threats. Through a blend of theoretical knowledge and practical applications, participants will gain an understanding of common cybersecurity threats, such as phishing and social engineering, while also examining the cognitive biases and psychological triggers that make these threats effective. Key topics include the psychology of decision-making under uncertainty, the impact of social influence on security practices, and strategies for fostering a security-first mindset in both personal and organizational contexts.

[View online](#)

Price: 20,00 €

Start date: 13.12.2024

Instructor(s): RAMADAN Omar

Language: English

Difficulty: Beginner





ETHICAL HACKING WITH ZENMAP: ESSENTIAL NETWORK SCANNING TECHNIQUES FOR ETHICAL HACKERS

This course is aimed at intermediate and advanced practitioners, and provides a comprehensive overview of one of the key phases in ethical hacking: network scanning, which is essential for gathering information about a target, such as a website or an organization's network. The course specifically focuses on Zenmap, the graphical user interface (GUI) version of Nmap, a powerful network scanning tool.

During this course, learners will gain a deep understanding of Zenmap's features and learn how to apply them in practical situations. They will explore how Zenmap operates within the OSI model, and gain the skills to set up and launch their own network scanning lab. Additionally, learners will analyze and apply various host discovery methods, port scanning techniques, and Zenmap's timing and scripting functionalities in real-world scenarios. This course equips learners with the knowledge and skills needed to effectively use Zenmap for network scanning tasks in ethical hacking.

[View online](#)

Price: 60,00 €

Start date: 25.10.2024

Instructor(s): ADAVOUDI Amir

Language: English

Difficulty: Intermediate



INTRODUCTION À LA CYBERSÉCURITÉ

Les technologies digitales et l'internet sont devenus indispensables dans la vie quotidienne.

De ce fait les attaques sur les systèmes d'information accroissent de jour en jour. Il est donc indispensable de connaître les méthodes et techniques des attaquants afin d'éviter des conséquences néfastes au niveau professionnel et privé.

Ce cours offre une vue globale sur les systèmes d'informations et prépare les participants aux problèmes qui peuvent survenir dans le quotidien.

Le cours présente un échange constant entre le formateur et les participants. La théorie est illustrée par des petites séquences vidéo qui amènent les participants à réfléchir et qui sera base de discussion pour trouver des solutions pour contourner l'attaque.

[View online](#)

Price: 36,00 €

Start date: 07.11.2024

Instructor(s): GNAD Christiane

Language: French

Difficulty: Beginner

INTRODUCTION TO THE DOMAIN NAME SYSTEM

This course proposes an introduction to the DNS, aimed at IT students, professionals or enthusiasts wishing to understand how the DNS works and administer their own domain name(s) and aims at giving them sound theoretical basis and a concrete hands-on experience to embrace best practices and avoid caveats in operation. It may also be suitable for people curious about the functioning of domain names on the Internet.

[View online](#)

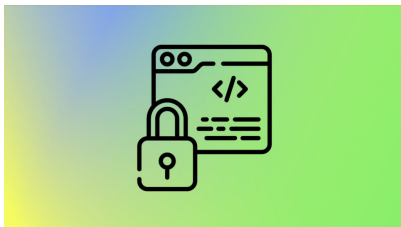
Price: 28,00 €

Start date: 15.11.2024

Instructor(s): Dr. HERBIET Guillaume-Jean

Language: English

Difficulty: Beginner



LEARNING TRACK - CYBERSECURITY ESSENTIALS

The learning track aims to develop participants' skills and knowledge of system and network administration in a cybersecurity context, including understanding the principles of system and network administration and learning methods to prevent and mitigate cyber attacks.

[View online](#)

Price: 528,00 €

Start date: 04.11.2024

Instructor(s): BRANDENBURGER Sharif, HOARAU Frédéric, JUNG Paul, MIESCH Olivier, PAIN Alexis, RIGHETTO Dominique

Language: English

Difficulty: Intermediate



MICROSOFT SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Ce cours fournit des connaissances de base sur les concepts de sécurité, de conformité et d'identité, ainsi que sur les solutions Microsoft basées sur le cloud qui s'y rapportent.

Le support de cours et l'environnement des labs est en anglais.

[View online](#)

Price: 28,00 €

Start date: 09.12.2024

Instructor(s): Microsoft Certified Trainer Xavier NIX

Language: French

Difficulty: Beginner



MODULE 2: NETWORK AND SECURITY – ADVANCED LEVEL

The second module in this Learning track extends from Module 1 and will focus on IT security operations within an enterprise corporate environment. This includes:

- Applications and services security, such as web applications, emails, databases, networks, WIFI, and authentication.
- Information systems security, vulnerability management
- Ethical hacking techniques and penetration testing
- Security incident management
- Incident response principles
- End-of-course project and preparation for SSCP or CompTIA Security+ certification

In covering daily operations, we will also address governance and best practices. The module provides for applying the acquired skills, validating learned knowledge and preparing for the certificates.

To successfully complete this module, it is strongly recommended to have completed [Module 1: Network and security – Introductory level](#) of this learning track.

[View online](#)

Price: 140,00 €

Start date: 11.11.2024
Instructor(s): Frédéric HOARAU
Language: English
Difficulty: Intermediate



MODULE 3: SECURITY INCIDENT MANAGEMENT

Preparing for incident management is essential in today's environment. This module includes:

- Principles of an incident
- The life cycle of a vulnerability
- Log management strategy
- Setting up detection systems
- Backup strategy

Learners will learn about the different stages of an incident, and how to prepare for them, including setting up a detection and response strategy, analysing logs, and managing backups. Questions answered in this module are: What is a vulnerability and its lifecycle? What is an incident, how to prevent it or detect it at early stage? What are the detections mechanisms and how to set them up? Why and how do we backup data? The outcome of completing this module successfully is to have the knowledge and skills to ensure the necessary defences and logs are in place before the incident occurs.

[View online](#)

Price: 12,00 €
Start date: 18.11.2024
Instructor(s): MIESCH Olivier
Language: English
Difficulty: Intermediate



MODULE 4: INCIDENT RESPONSE PRINCIPLE

The course will focus on understanding an incident lifecycle and to review for each step the preparation, handling and technical objectives of each phase.

Managing an incident happens during stressful moments for IT operations. Preparation and processes are mandatory to be able to handle such situation. Therefore, we will focus on understanding an incident lifecycle and to review for each step the preparation, handling and technical objectives of each phase.

This is a short, theoretical module, in which you will learn about the different stages of an incident, and how to prepare for them, including setting up a detection and response strategy, analysing logs, and managing backups.

[View online](#)

Price: 12,00 €

Start date: 18.11.2024

Instructor(s): Paul JUNG

Language: English

Difficulty: Intermediate



MODULE 5 - PART 1: APPLICATION SECURITY - LEVEL 1 - INTRODUCTION TO SECURE CODING

As technology becomes increasingly ubiquitous in our daily lives, the need for secure applications becomes ever more important. This course is an introduction to application security for developers, covering a range of topics from common attacks and defences to secure coding principles and specific security controls.

This module introduces learners to the defensive side of Application Security. In this course, you'll learn the basics of web application architecture and the threat landscape. You'll explore common attacks, such as those on the OWASP Top 10 list, and discover defence mechanisms for mitigating these threats.

The principles and practices of secure coding will be highlighted, including the principle of least privilege and the importance of security testing during development. We'll also look at specific security controls, such as authentication, session management, authorization, input validation and output coding, error handling and logging, file system access, cryptography and defensive browser functions. A Review of secdevops principles will also be

covered.

By the end of the course, you will have a fundamental understanding of application security and best practices for ensuring that the applications you develop are secure. This course assumes a basic understanding of web development principles and programming concepts, with prior experience in a programming language recommended.

[View online](#)

Price: 28,00 €

Start date: 19.11.2024

Instructor(s): PAIN Alexis

Language: English

Difficulty: Intermediate



MODULE 5 – PART 1: APPLICATION SECURITY – LEVEL 2 – ATTACKS AND DEFENSES IN ACTION

This module addresses different kinds of application vulnerabilities and different kinds of vulnerabilities specific to API and web services.

The module covers:

- Different types of vulnerabilities that are commonly present in applications
- How to detect them
- How to validate them
- How to fix them
- Different types of vulnerabilities that are commonly present in API
- How to detect them
- How to validate them

[View online](#)

Price: 28,00 €

Start date: 20.11.2024

Instructor(s): RIGHETTO Dominique

Language: English

Difficulty: Intermediate



MODULE 5 – PART 1: APPLICATION SECURITY – LEVEL 3 – INTRODUCTION TO APPLICATION SECURITY AUDITS

The objective of this training is to allow the students to discover the offensive side of the Application Security about Web Application and practice it during a lab and the offensive side of Mobile Application security and practice it during a lab.

During this training, the students will discover:

- What is a Web Application Vulnerability Assessment?
- The different steps of this kind of assessment;
- The methodology used to rate the security issues;
- The open referential that can be used to conduct an assessment.
- What is a Mobile Application Vulnerability Assessment?
- The different steps of this kind of assessment;
- The methodology used to rate the security issues;
- The open referential that can be used to conduct an assessment.

[View online](#)

Price: 28,00 €

Start date: 21.11.2024

Instructor(s): RIGHETTO Dominique

Language: English

Difficulty: Advanced



MODULE 5 – PART 2 : DEVOPS AND PIPELINE SECURITY

DevSecOps training is a practical, course designed to integrate security into your DevOps pipeline. It focuses on real-world scenarios and tools like GitLab CI/Actions/Jenkins, Kafka, Grafana, Terraform, and Kubernetes to highlight vulnerabilities and best practices.

Securing the DevOps Pipeline: A Practical Guide to DevSecOps

In today's fast-paced digital landscape, delivering software rapidly and securely is no longer a luxury it's a necessity. Organizations are under increasing pressure to push features and updates while ensuring that security is baked into every part of the development process. This 14-hour, hands-on

DevSecOps training is designed to help you integrate security practices into your DevOps pipeline, enhancing your ability to detect and mitigate vulnerabilities without slowing down development.

This course is not a theoretical deep dive; it's an immersive, practical experience where you'll configure and secure real-world environments using popular tools like Jenkins, GitLab CI, Kafka, Grafana, Terraform, Kubernetes, and more. Throughout the course, you will encounter common vulnerabilities and misconfigurations, learn to identify them, and implement security solutions in real time.

[View online](#)

Price: 56,00 €

Start date: 25.11.2024

Instructor(s): BRANDENBURGER Sharif

Language: English

Difficulty: Intermediate



MODULE 6: MALWARE AND FORENSICS

Preparing for incident management is essential in today's environment. In this module, students will learn about the different stages of an incident, and how to prepare for them. Setting up a detection and response strategy, analysing logs, managing backups. Using a case study, we will dig into the key concepts and technical approaches to adopt in handling cybersecurity incidents.

Case study : Ransomware attack

In this scenario, the information system was breached by exploiting a remote access vulnerability several months ago. The attacker took control of the information system, exfiltrated data and then deployed a ransomware attack across the entire infrastructure. Finally, he published the stolen data publicly. Explanation of the underground ecosystem. We will use a similar scenario and perform an incident response.

[View online](#)

Price: 84,00 €

Start date: 28.11.2024

Instructor(s): JUNG Paul

Language: English

Difficulty: Advanced



MULTI-FACTOR AUTHENTICATION

This course presents various methods of multi-factor authentication to the participants. During this hands-on course, participants will learn how multi-factor authentication works and how they can secure their account by adding an additional factor.

[View online](#)

Price: 12,00 €

Start date: 07.10.2024

Instructor(s): Winter Stefan

Language: English

Difficulty: Beginner



NETWORK SECURITY AND INTRO TO THREAT HUNTING WITH WIRESHARK

This course is an introduction to using Wireshark for network security. It includes practical exercises about Transport Layer Security and analysis of malware communication.

[View online](#)

Price: 36,00 €

Start date: 03.10.2024

Instructor(s): Dr HOMMES Stefan

Language: English

Difficulty: Intermediate



OPERATING A DNS AUTHORITATIVE SERVICE

This course is aimed at IT students, professionals or enthusiasts wishing to operate their own DNS authoritative servers in order to publish domain name(s). It will give them sound theoretical basis and a concrete hands-on experience to embrace best practices, troubleshoot issues and avoid caveats in operation.

[View online](#)

Price: 28,00 €

Start date: 22.11.2024

Instructor(s): Dr. HERBIET Guillaume-Jean

Language: English

Difficulty: Intermediate



OPERATING A DNS RESOLUTION SERVICE

This course is aimed at IT students, professionals or enthusiasts wishing to operate their own DNS resolvers in order to provide a name resolution service to their personal, corporate or institutional network. It will provide sound theoretical basis and a concrete hands-on experience to embrace best practices, troubleshoot issues and avoid caveats in operation.

[View online](#)

Price: 28,00 €

Start date: 29.11.2024

Instructor(s): Dr. HERBIET Guillaume-Jean

Language: English

Difficulty: Intermediate



PRINCIPLES OF THE DOMAIN NAME SYSTEM SECURITY EXTENSIONS (DNSSEC)

Domain Name System Security Extensions (DNSSEC) adds origin authentication and integrity protection to the protocol by signing DNS data. However the ratio of signed domain names remains low, mostly because, as any security feature, DNSSEC brings some risks when implemented without a proper understanding.

This course targets IT students, professionals or enthusiasts currently managing domain names and willing to start signing their DNS zones, improve or gain confidence in their signing procedures with hands-on experience and best-practices.

[View online](#)

Price: 28,00 €

Start date: 06.12.2024

Instructor(s): Dr. HERBIET Guillaume-Jean

Language: English

Difficulty: Intermediate



SENSIBILISATION À LA SÉCURITÉ DE L'INFORMATION

Cette formation de sensibilisation initie les participants aux risques liés aux ordinateurs, aux appareils mobiles et à l'internet. En ce qui concerne les violations de données et les cyberattaques, ce sont surtout les personnes qui sont visées par les cybercriminels, et non les ordinateurs. À l'aide de nombreux exemples concrets, la session interactive vise à confronter les participants à des menaces auxquelles ils seront confrontés dans la vie de tous les jours, et à leur apprendre à maîtriser ces situations. Les participants qui auront suivi la formation seront beaucoup plus résistants face à ces cyber-risques.

[View online](#)

Price: 12,00 €

Start date: 05.11.2024

Instructor(s): Muller, Steve

Language: French

Difficulty: Beginner



TCP/IP DEEP DIVE FOR PRACTITIONERS WITH WIRESHARK

This course will provide you with an explanation of important internet and TCP/IP protocols by going through practical exercises using Wireshark for each protocol. The course will also explain Wireshark GUI and its functionality for packet analysis.

[View online](#)

Price: 48,00 €

Start date: 29.11.2024

Instructor(s): Dr. HOMMES Stefan

Language: English

Difficulty: Intermediate